IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer program product embodied on a computer readable medium for controlling a computer to scan a compressed computer file for malware, said compressed computer file being compressed using a compression algorithm, said computer program product comprising:

comparison code operable to compare a plurality of compressed malware signatures compressed using said compression algorithm with said compressed computer file to identify malware within said compressed computer file;

detection code operable to detect from a compressed computer file to be scanned what compression algorithm has been used to compress said compressed computer file; and

compression code operable to compress a plurality of uncompressed malware signatures using said detected compression algorithm to generate said plurality of compressed malware signatures.

2. (Cancelled)

3. (Currently Amended) A computer program product as claimed in claim [2]1, wherein said detection code reads compression algorithm specifying data from said compressed computer file.

4. (Original) A computer program product as claimed in claim 3, wherein said compression algorithm uses Huffman coding and said compression algorithm specifying data includes a Huffman coding table used to compressed said compressed computer file.

5. (Original) A computer program product as claimed in claim 1, wherein said comparison code uses a Boyer Moore algorithm or an algorithm based upon structuring the signatures in a tree.

6. (Original) A computer program product as claimed in claim 1, wherein said malware includes at least one of computer viruses, Trojans, worms, banned files and e-mails containing banned content.

7. (Currently Amended) A method of scanning a compressed computer file for malware, said compressed computer file being compressed using a compression algorithm, said method comprising the step of:

comparing a plurality of compressed malware signatures compressed using said compression algorithm with said compressed computer file to identify malware within said compressed computer file;

detecting from a compressed computer file to be scanned what compression algorithm has been used to compress said compressed computer file; and

compressing a plurality of uncompressed malware signatures using said detected compression algorithm to generate said plurality of compressed malware signatures.

8. (Cancelled)

9. (Currently Amended) A method as claimed in claim [8]7, wherein said step of detecting reads compression algorithm specifying data from said compressed computer file.

10. (Original) A method as claimed in claim 9, wherein said compression algorithm uses Huffman coding and said compression algorithm specifying data includes a Huffman coding table used to compressed said compressed computer file.

11. (Original) A method as claimed in claim 7, wherein said step of comparing uses a Boyer Moore algorithm or an algorithm based upon structuring the signatures in a tree.

12. (Original) A method as claimed in claim 7, wherein said malware includes at least one of computer viruses, Trojans, worms, banned files and e-mails containing banned content.

13. (Currently Amended) Apparatus for scanning a compressed computer file for malware, said compressed computer file being compressed using a compression algorithm, said apparatus comprising:

comparison logic operable to compare a plurality of compressed malware signatures compressed using said compression algorithm with said compressed computer file to identify malware within said compressed computer file;

detection logic operable to detect from a compressed computer file to be scanned what compression algorithm has been used to compress said compressed computer file; and

compression logic operable to compress a plurality of uncompressed malware signatures using said detected compression algorithm to generate said plurality of compressed malware signatures.

14. (Cancelled)

15. (Currently Amended) Apparatus as claimed in claim [14]13, wherein said detection logic reads compression algorithm specifying data from said compressed computer file.

16. (Original) Apparatus as claimed in claim 15, wherein said compression algorithm uses Huffman coding and said compression algorithm specifying data includes a Huffman coding table used to compressed said compressed computer file.

17. (Original) Apparatus as claimed in claim 13, wherein said comparison code uses a Boyer Moore algorithm or an algorithm based upon structuring the signatures in a tree.

18. (Original) Apparatus as claimed in claim 13, wherein said malware includes at least one of computer viruses, Trojans, worms, banned files and e-mails containing banned content.